AGCT-14 Conference

Arithmetic, Geometry, Cryptography and Coding Theory

June 3rd-7th 2013

C.I.R.M. - France

Stéphane Ballet, Marc Perret and Alexey Zaytsev

Program and abstracts

	Monday	Tuesday	Wednesday	Thursday	Friday
9.00 - 10.00	Lauter	Ghorpade	Li	Schmidt	Rolland
10.00 - 10.30	Kohel	Hansen	Hallouin	Belliard	Lachaud
10.30- 11.00	CB	CB	CB	CB	CB
11.00 - 11h30	Ducet	Kabatiansky	Bassa	Rokaeus	Haloui
11.30 - 12h00		Tukumuli	Beelen	Poinsot	Homma
12.30- 14.00	Lunch	Lunch	Lunch	Lunch	Lunch
14.00 - 14.30			Free		Kawakita
14.30 - 15.00					Kubrac
15.00 - 15.30					Final Coffee
16.00 - 17.00	Nart	Randriam		Rybakov	
17.00- 17.30	Goncalves	Smith		Ritzenthaler	
17.30- 18.00	CB	CB		CB	
18.00- 18.30	Caullery	Diem	Afternoon	Boyer	
18.30- 19.00	Ozbudak	Sijsling		Bruin	
19.30-	Diner	Diner	Diner	Conference diner	

CB: Coffee Break.

Free Afternoon: walk in the calanques (Morgiou+Sugiton) or football match.

Abstracts.

Alp Bassa: Rational points on curves over finite fields and Drinfeld modular varieties. In the past modular curves of various type (classical, Drinfeld, Shimura) have been used successfully to construct high genus curves with many rational points over finite fields of square cardinality. In this talk I will explain how Drinfeld modular varieties can be used similarly to obtain high genus curves with many rational points over any non-prime finite field. This way we obtain lower bounds for the Ihara constant $A(q)$ for all non-prime q, which are better then all previously known bounds.

This is joint work with Beelen, Garcia, Stichtenoth.

Peter Beelen: Modular towers obtained using Drinfeld modules. This talk is a continuation of the talk by Alp Bassa. Some variations of the modular construction of towers explained by Alp Bassa will be given. One possibility is to vary the characteristic of the Drinfeld modules, but also a variation of the base ring is used to produce more examples of asymptotically good Drinfeld modular towers. Some explicit examples will be given in case the ring is the coordinate ring of an elliptic curve in Weierstrass form.

The work is joint with Alp Bassa and Nhut Nguyen.

Jean-Robert Belliard: On annihilation of real classes. Let F be a number field, abelian over $\mathbb{Q}$ and let p be a prime totally split in F. I will present a proof that Solomon's ψ_F element annihilates the torsion of the Galois group of the maximal abelian p-ramified p-extension of F . This statement is stronger than conjecture 4.1 of Solomon [On a construction of p-units in abelian fields. Invent. Math. 109 (1992), no.2, 329-350.]

This is a joint work with Anthony Martin.

Yvan Boyer: Families of genus 3 hyperelliptic curves whose jacobians are $2-2-2$ isogenous. In genus two, for each curve it's well-known that we can construct another curve such that their jacobians are $2-2$ isogenous. In genus three, it's no longer true. Thanks to theta functions and the duplication formula, we can find exactly four 4-parameters families of genus 3 hyperelliptic curves H whose jacobian is a $2-2-2$ isogenous to the jacobian of an hyperelliptic curve H'. For two of these families, the curves H and H' belong to the same family. This talk is devoted to the two other families for which we can explicitly compute the curves with a correspondence between them, commuting with the hyperelliptic involution.

Niels Bruin: $(3,3)$ - descent on Jacobians on genus 2 curves. We characterize genus 2 curves with a particular partial 3-level structure on their Jacobians and describe how to do a 3-isogeny descent on them. This allows us to prove the presence of 3-torsion in the Tate-Shafarevich groups of some genus 2 jacobians.

This is joint work with Victor Flynn and Damiano Testa.

Florian Caullery: On the conjecture about Exceptional Almost Perfectly Nonlinear functions. In this talk we show that there is no vectorial Boolean function of degree $4e$ with $e \equiv 3 \ (mod\ 4)$ which is APN over infinitely many extensions of its field of definition. This proof use tools of algebraic geometry and more especially the Lang Weil bound. It is a new step in the proof of the conjecture of Aubry, McGuire and Rodier.

Klauss Diem: Special linear systems on curves and the discrete logarithm problem. We consider the discrete logarithm problem for curves of a fixed genus. One observes that for the resolution of the problem with the index calculus method, it is advantageous to consider special linear systems (or series) on a given curve. The following questions thus pose thmselves:

- Which special linear systems do curves generally have?
- How can one generate them efficiently?

In the talk these questions will be addressed.

Virgile Ducet: Number of rational points of Shimura curves over finite fields. The modular curves $X_0(N)$ form a class of curves with a rich arithmetic theory; in particular, sequences of such curves over a finite field and with asymptotically growing genus turn out to be optimal, in the sense that they reach the Drinfel'd-Vlădut bound. In this talk we will be interested in arithmetic aspects of the Shimura curves $X_0^{\mathfrak{D}}(\mathfrak{N})$, which are natural generalizations of the curves $X_0(N)$, with the idea of looking at the asymptotic behavior of the number of points of their reduction over a finite field.

Cecile Goncalvez: A point counting algorithm for cyclic covers of the projective line. Computing the zeta function of curves over finite fields is an important problem in computational algebraic geometry and has many applications in cryptography and number theory. The first deterministic polynomial-time point-counting algorithm was introduced early in the eighties by Schoof [Sch85], but this algorithm is only available in small genus. In 2001, Kedlaya [Ked01] provided the first point-counting algorithm practicable in genus greater than 2. Using Monsky-Washnitzer cohomology, this algorithm computes the zeta function of a hyperelliptic curve in odd characteristic in polynomial time. In this talk, we will present an algorithm for counting points on cyclic cover of the projective line $y^r = f(x)$ over a finite field $\mathbb{F}_q$, with r and the degree of f not necessarilly coprime, in characteristic which does not divide r. This is an extension of Gaudry and Gurel's algorithm [GG01] for superelliptic curves. The complexity, assuming r and the genus are fixed, is $O(\log 3q)$ in time and space, just like for superelliptic curves. Our first implementation in Magma allows us to compute some zeta functions of interesting curves that we were not able to compute before. As an application, we prove the absolute simplicity of some families of Jacobians of interest in number theory, extending some results of [Smi11].

Sudhir Ghorpade, plenary talk: Linear codes related to Grassmann varieties. I will give an outline of several recent and not-so-recent results concerning Grassmann codes, Schubert codes, and affine Grassmann codes.

Emmanuel Hallouin: Recursive towers of curves over finite fields and graphs. We present new tools for both theoretic and explicit study of the asymptotic behavior of a recursive tower of curves over a finite field. The key point consists in associating an infinite directed graph to the tower. We illustrate how this graph can help for the explicit study of a concrete tower. Then, we prove some specific properties satisfied by the graph. In turn, the graph permits to prove a result about the general behavior of a recursive tower.

This is a joint work with Marc Perret.

Safia Haloui: On the number of rationals points on Prym varieties over finite fields. We give upper and lower bounds for the number of rational points on Prym varieties over finite fields which improve the ones of Perret. Moreover, we determine the exact maximum and minimum number of rational points on Prym varieties of dimension 2.

This is a joint work with Yves Aubry.

Johan P. Hansen: Osculating spaces of varieties and linear network codes. Algebraic varieties have in general an osculating structure. By Terracini's lemma [Ter11] their embedded tangent spaces tend to be in general position. Specifically, the tangent space at a generic point $P \in Q1Q2$ on the secant variety of points on some secant is spanned by the tangentspaces at Q_1 and Q_2. In general the secant variety of points on some secant have the expected maximal dimension and therefore the tangent spaces generically span a space of maximal dimension [Zak93]. In [Han12b], [Han12a] and [Han13] we suggest osculating spaces and tangent spaces of algebraic varieties as a source for constructing linear subspaces in general position of interest for linear network coding. In particular we present the osculating subspaces of Veronese varieties and apply them to obtain linear network codes. Linear network coding transmits information in terms of a basis of a vector space and the information is received as a basis of a possible altered vector space. Ralf ! Koetter and Frank R. Kschischang [KK08] introduced a metric on the set af vector spaces and showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of

the transmitted and received vector space is suficiently large. The proposed osculating spaces of Veronese varieties are equidistant in the above metric. The parameters of the resulting linear network codes are determined.

Masaaki Homma: The characterization of Hermitian surfaces by the number of points. The nonsingular Hermitian surface of degree $\sqrt{q}+1$ is characterized by its number of $\mathbb{F}_q$-points. Namely, we prove the following theorem.
Theorem. An absolutely irreducible surface over $\mathbb{F}_q$ of degree $\sqrt{q}+1$ in $\mathbb{P}^3$ which has $(q+1)(\sqrt{q^3}+1)$ points over $\mathbb{F}_q$ is a nonsingular Hermitian surface.

This is a joint work with Seon Jeong Kim.

Grigori Kabatiansky: Error-correcting codes over real numbers and compressed sensing: an overview and slightly beyond. The term "Compressed Sensing" (CS) was coined by D. L. Donoho in his article with the same title that appeared in IEEE Transactions on Information Theory (2006). He showed that n-dimensional vectors having a few "significant" coordinates can be recovered from a small number of measurements. The topic was immediately (or independently) pursued by E. J. Candes and Terence Tao, who showed the connection between this problem and the well-know problem on almost isometric embedding of normed spaces, and the work commenced. The same two authors discussed in the paper "Decoding by linear programming" the relationship of CS and error-correction over the field of real numbers. These topics become particularly popular because of the fact that one of its principal ingredients is $L1$-optimization, which has already become popular in various applications (thanks in particular to the LASSO method). We will provide an accessible review of the main results in this field, established some links with its discrete analogs and give a more adequate model of error-correcting codes over real numbers.

Motoko Kawakita In 1970s Goppa discovered algebraic-geometric codes, where we need explicit curves with many rational points to construct good codes. Recently I found that the sextics, defined by Wiman in 1896 and by Edge in 1981, attain the Hasse-Weil-Serre bound over some finite fields of order p, p^2 or p^3, for a prime number p. For some sextics among them, we determined the precise condition on the finite field over which the sextics attain the Hasse-Weil-Serre bound. Also I updated many entries in manYPoints.org by computer search. This talk contains some extensions of my paper "Wiman's and Edge's sextic attaining Serre's bound". http://www.manypoints.org/upload/kawakita.pdf

David Kohel: The geometry of efficient arithmetic on elliptic curves. The arithmetic of elliptic curves, namely addition and scalar multiplication, can be described in terms of global sections of line bundles on $E\times E$ and E, respectively. By means of a study of the finite dimensional vector spaces of global sections, we show how to determine and classify efficiently computable polynomial maps defining the addition morphism as a rational map (addition laws) and globally defining a morphism $[n]$ of scalar multiplication.

Mitya Kubrak: Brauer-Siegel type theorems for reductive groups. Classical Brauer-Siegel theorem gives the asymptotic for the order of the class group of a number field K in terms of its discriminant if the degree of K over $\mathbb{Q}$ is bounded. It was generalized by Tsfasman and Vladuts: to write down the asymptotic you really do not need the boundness of the degrees, you need the family of fields to be *asymptotically exact*. I will tell you about the further generalization of their formula firstly to the case of arbitrary algebraic torus and its pullbacks on ass. exact family, which is former Kunyavskii-Tsfasman conjecture, and secondly to the case of any reductive group G which in the functional case gives the asymptotic to the number of point on the moduli stack of G-bundles.

Gilles Lachaud: On the number of points on abelian and jacobian varieties over finite fields. We give upper and lower bounds for the number of points on abelian varieties over finite fields, and lower bounds specific to Jacobian varieties. We also determine exact formulas for the maximum and minimum number of points on Jacobian surfaces.

This is a joint work with Yves Aubry and Safia Haloui.

Kristin Lauter, plenary talk: On a Generalization of Gross-Zagier and applications to Genus 2 Curves in Cryptography . The modular j-function plays an important role in number theory: its values at quadratic imaginary integers are called singular moduli. Singular moduli can be interpreted as an invariant of CM elliptic curves and play a role in explicit class field theory. In 1985, Gross and Zagier gave an elegant formula for the factorization of norms of differences of singular moduli associated to a pair of imaginary quadratic discriminants d1 and d2, under the assumption that d1 and d2 are fundamental and relatively prime. Their theorem was one of the ingredients in the proof of the only known case of the Birch-Swinnerton Dyer Conjecture. This talk will present a generalization of their result to give a complete factorization for any two fundamental discriminants which are not necessarily coprime, and obtain at least a partial factorization for any two quadratic imaginary discriminants. We will discuss the motivation for this generalization arising in cryptography and give an application to proving an intersection formula on Hilbert modular surfaces related to the work of Bruinier and Yang. This is joint work with Bianca Viray.

Winnie Li, plenary talk: Towers of Ramanujan graphs. A d-regular graph is Ramanujan if its nontrivial eigenvalues in absolute value are bounded by $2\sqrt{d-1}$. By means of number-theoretic methods, infinite families of Ramanujan graphs were constructed by Margulis and independently by Lubotzky-Phillips-Sarnak in 1980's for $d = q + 1$, where q is a prime power. The existence of an infinite family of Ramanujan graphs for arbitrary d has been an open question since then. Recently Adam Marcus, Daniel Spielman and Nikhil Srivastava gave a positive answer to this question by showing that any bipartite d-regular Ramanujan graph has a 2-fold cover that is also Ramanujan. In this talk we shall discuss their approach and mention similarities with function field towers.

Enric Nart, plenary talk: Genetics of polynomials over local fields. Let P be the set of monic irreducible separable polynomials with coefficients in the ring of integers $\mathcal{O}$ of a local field. Let m be the maximal ideal of $\mathcal{O}$. A computer cannot manipulate (or even store) the polynomials F in P with infinite precision. Only representatives $\varphi \in 2F + m^n$ in a certain class modulo a power of m can be considered in practice. We present in this talk an equivalence relation (Okutsu equivalence) on the set P such that the quotient set has the structure of a tree which may be described in terms of discrete invariants. This leads to computational representations of the elements of P of the form $(t; \varphi)$ where t is the collection of discrete invariants correponding to the class $[F]$, and $\varphi \in [F]$ has coefficients in some discrete ring. We say that $(t; \varphi)$ is an OM representation of F. The ingredients (t, φ) are a kind of " algebraic" and "analytic" part of the computational representation of F. The algebraic part t, which is called the *type* of F, is a kind of DNA sequence, common to all individuals in $[F]$. The Montes algorithm computes OM representations of the irreducible factors of a separable polynomial in $\mathcal{O}[x]$. At the input of one such OM representation, the Single-factor lifting algorithm derives an approximation with prescribed precision to the corresponding irreducible factor. These two algorithms are the basis of a series of fast routines to solve several arithmetic tasks in number fields and global function fields.

This is a joint work with Jordi Guàrdia.

Ferruh Ozbudak: Perfect nonlinear maps from $\mathbb{F}_{q^3}$ to $\mathbb{F}_{q^2}$. We present some results on some perfect nonlinear maps from $\mathbb{F}_{q^3}$ to $\mathbb{F}_{q^2}$. There are some connections to cryptography, semifields and algebraic curves over finite fields.

This is a joint work with Alexander Pott.

Laurent Poinsot: Moduli space of pairings on roots of unity. This talk is about the problem of classification of pairings up to isomorphism. Bilinear maps with values on a given abelian group form a cocartesian category and thus the object class of its skeleton is a commutative monoid of which pairings form a sub-monoid. When the domain of bilinear maps is restricted to finite abelian groups, the monoid of (equivalence classes under isomorphism of) pairings satisfies a local finiteness property, namely the fact that each pairing admits only finitely many decompositions with non-trivial factors, that makes possible to consider the problem of classification of pairings (up to isomorphism) by mean of generators. If the codomain of bilinear maps is the group of complex roots of unity, then this classification appears to be very simple.

Karl Rokaeus: Curves with many points over finite fields. We search for curves with many rational points over a finite field. By starting with a curve of low genus, the aim is to use class field theory to search through all abelian covers of this curve of genus up to 50. This gives many curves with more points than was previously known to exist, and also reproduces almost all of the best known curves. The complete search through all abelian covers is possible for some base curves over $GF(2)$.

Hugues Randriambololona, plenary talk: On products and powers of codes under componentwise multiplication. We will be interested in the operation which, to two linear codes C, C' of same length, attaches the linear code $C * C'$ spanned by componentwise products of their codewords - and when iterated, allows to define powers of a code. These are very natural constructions, both from the point of view of classical coding theory, as well as from the perspective of algebraic geometry. We will study the structure, symmetries, and give upper and lower bounds on the parameters of the codes thus constructed. Most of these results are very basic, although a few of them are slightly more elaborate. If time permits, we will also look at links with the theory of tensor rank and multilinear algorithms.

Christophe Ritzenthaler: Distribution of genus 3 curves over finite fields according to their trace. Presenting some numerical evidences, we'd like to convince the audience that there seem to be unknown phenomenas structuring the distribution of isomorphism classes of genus 3 curves over finite fields with respect to their trace.

Robert Rolland, plenary talk: Lower bounds on the number of rational points of Jacobians over finite fields and application to algebraic function fields in towers.

Abstract: We give effective bounds for the class number of any algebraic function field of genus g defined over a finite field. These bounds depend on the possibly partial information on the number of places on each degree $\leq g$. Such bounds are especially useful for estimating the class number of function fields in towers of function fields over finite fields. We give examples in the case of asymptotically good towers. In particular we estimate the class number of function fields which are steps of towers having one or several positive Tsfasman-Vladut invariants. Note that the study is not done asymptotically, but for each individual step of the towers for which we determine precise parameters .

This is a joint work with Stéphane Ballet and Seher Tutdere.

Sergey Rybakov, plenary talk: Groups of points on abelian varieties over finite fields. Let X be an algebraic variety over a finite field k. The set $X(k)$ of points defined over k is an important invariant of X. If X is an abelian variety, then $X(k)$ is a finite abelian group. Tsfasman classified finite abelian groups which can be realized as groups of points on elliptic curves over finite fields. Rueck and Voloch obtained the same result independently using results of Schoof. It is important that for the classification in question one first divide the set of elliptic curves into isogeny classes and then classify groups of points inside a given isogeny class. By the Tate-Honda theorem, isogeny class of abelian varieties of arbitrary dimension over finite field corresponds to characteristic polynomial of Frobenius action on the ℓ-th Tate module of any variety from the class (Weil polynomials). These polynomials are known for abelian varieties of low dimensions. The talk is devoted to some recent results on the structure of the groups points in d! imensions 2 and 3.

Alexander Schmidt, plenary talk: a survey on higher dimensional class field theory. We give a survey on higher dimensional class field theory for regular schemes of finite type over Spec($\mathbb{Z}$). We start by explaining the now classical approach of Kato/Saito using Milnor K-sheaves. Then we explain the cycle theoretic approach of Schmidt/Spiess, which describes the maximal tame factor group of the abelianized fundamental group and the approach of Wiesend, which removes the tameness assumption in the mixed characteristic case. If there is time, we will present two recent developments for schemes of finite type over finite fields: the description of wild coverings of regular varieties by Kerz/Saito and the description of tame coverings of singular varieties by Geisser/Schmidt.

Jeroen Sijsling: Isomorphisms of plane quartics. We discuss ways to quickly determine the isomorphisms between two smooth quartic plane cures. The main method uses previous results by Sander van

Rijnswou and employs covariants of ternary quartic forms. A considerable speed-up, in particular over finite fields, is obtained by using the theory of quaternion algebras. For substrata of the moduli space with big automorphism group, we use hyperflex configurations for an alternative effective approach.

Benjamin Smith: Families of efficient endomorphisms on elliptic curves from $\mathbb{Q}$-curves. Scalar multiplication (that is, exponentiation) on elliptic curves over finite fields is a key operation in many modern asymmetric cryptographic primitives. Gallant, Lambert, and Vanstone showed that if an elliptic curve has an efficiently computable endomorphism, then the endomorphism can be used to accelerate scalar multiplication on the curve, leading in turn to faster encryption and decryption operations.

In this work, we use the theory of $\mathbb{Q}$-curves to construct a series of new geometric families of elliptic curves with efficient endomorphisms amenable to GLV-style scalar multiplication algorithms. Our families form a natural generalization of Galbraith-Lin-Scott (GLS) curves, while neatly avoiding their inherent vulnerability to the Fouque-Lercier-Réal-Valette fault attack.

Tukumuli Milakulo: On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields. We indicate a strategy in order to construct bilinear multiplication algorithms of type Chudnovsky in large extensions of any finite field. In particular, by using the symmetric version of the generalization of Randriambololona specialized on the elliptic curves, we show that it is possible to construct such algorithms with low bilinear complexity. More precisely, if we only consider the Chudnovsky-type algorithms of type symmetric elliptic, we show that the symmetric bilinear complexity of these algorithms is in $O(n(2q)^{\log_q^*(n)})$ where n corresponds to the extension degree, and $\log_q^*(n)$ is the iterated logarithm. Moreover, we show that the construction of such algorithms can be done in time polynomial in n.

This is a joint work with Stéphane Ballet et Alexis Bonnecaze.